IPS Engine for FortiOS - Release Notes

Version 6.2

FORTINET DOCUMENT LIBRARY
https://docs.fortinet.com

FORTINET VIDEO GUIDE
https://video.fortinet.com

FORTINET BLOG
https://blog.fortinet.com

CUSTOMER SERVICE & SUPPORT
https://support.fortinet.com

FORTINET TRAINING & CERTIFICATION PROGRAM
https://www.fortinet.com/support-and-training/training.html

NSE INSTITUTE
https://training.fortinet.com

FORTIGUARD CENTER
https://fortiguard.com/

END USER LICENSE AGREEMENT
https://www.fortinet.com/doc/legal/EULA.pdf

FEEDBACK
Email: techdoc@fortinet.com

February 10, 2021
IPS Engine for FortiOS 6.2 Release Notes
43-620-695647-20210210

TABLE OF CONTENTS

Change log

Date	Change Description
2021-02-10	Initial release.

Introduction

This document provides the following information for the Fortinet IPS Engine 6.2 build 071.

IPS Engine for FortiOS 6.2 build 071 is a release to FortiGuard. It is not a built-in release for FortiOS.

For additional FortiOS documentation, see the Fortinet Document Library.

What's new in IPS Engine 6.2 build 071

Bug ID	Description

641524	Added interface selection for IPS TLS protocol active probing.
	Problem: The TLS active probe must initiate connections from the FortiGate itself. For some transparent VDOMs that do not have the proper routing, the probe attempts fail.
	Solution: Customers can configure outgoing interface, source IP address, and VDOM for the IPS TLS active probe connection.
	CLI Changes:
	Add: Add interface selection for IPS TLS protocol active probing.
	Details:
	`config ips global`
	`  config tls-active-probe`
	`  set interface-selection-method <auto|sdwan|specify>`
	`  set interface <intf name> - when method is specify`
	`  set vdom <vdom name> - when method is sdwan or specify`
	`  set source-ip <source_ipv4> - when method is sdwan or specify`
	`  set source-ip6 <source_ipv6> - when method is sdwan or specify`
	`  end`
	`end`

On FortiGate, the engine version displays as 6.00071.

Product integration and support

The following table lists IPS engine product integration and support information:

FortiOS	6.4.0 and later

Resolved issues

The resolved issues listed below do not list every bug that has been corrected with this release. For inquiries about a particular bug, contact Customer Service & Support.

Bug ID	Description
539833	FortiGate 3100D cluster running IPS engine 04.029/04.030 causes high CPU usage on RTSP traffic and crashes with signal 7.
565955	Possible memory leak with IPS engine on FortiGate 1500D.
595659	IPS engine 5.00035 causes signal 11 crash.
621677	In flow-based mode improper rating classification when using HTTPS IP URL, with proceeding on the warning page does not work as expected.
624928	IPS engine 3.561 causes signal 11 crash.
625371	Crash on derived packet processing.
637084	Use existing private keys in FortiGate for certificate resigning.
637553	Web Filter produces rating error logs despite FortiGuard connectivity seemingly working correctly.
645848	FortiOS provides self-signed CA certificate intermittently with flow-based SSL certificate inspection.
646961	Explicit FTPS data channel cannot be established through policy when inspection mode is flow with antivirus enabled.
654363	Traffic logs shows "policy violation" for the traffic hitting the allow policy in NGFW policy mode.
654687	IPS engine causes segmentation fault in NGFW policy mode.
656300	IPS engine 6.032 has signal 11 crash at ips_latest_cfg on fortidemo test bed.
656687	Losing connection to RD gateway when adding or removing firewall policy.
658257	Firewall blocks STARTTLS-SMTP traffic when certificate inspection (proxy mode) and IPS sensor are enabled in a policy.
658482	High memory on IPS monitor/IPS engine.
660489	flow-based mode certificate inspection skips Web Filter URL filter check if SNI is not present in TLS client hello.
662573	IPS engine 5.000218 has several signal 11 crashes.
662785	Signatures for services other than SSL traffic with action "drop" is triggered as "detected" on SSL traffic.
662964	PCAP from IPS is not dumped as confirmed in packet-log-history/packet-log-post-attack.

Bug ID	Description
664728	Traffic fails for NGFW policy-based mode when TCP source port range includes zero value.
666025	IPS engine 6.00055 and 6.00054 have lots of signal 11 crashes at urc_find on corporate firewall.
667741	IPS engine v6.0.9 sb8878 causes memory leak after upgrade.
668486	Peer resets connection when visiting a URL in FortiGuard category with override action after clearing server cache.
668891	NGFW policy mode allows all services when selecting the ICMP service in security policy.
669138	IPS engine 4.067 crashes with segmentation fault and alarm clock.
670914	FortiGate 6301F cannot properly perform SSL inspection in flow-based mode policies.
671873	IPS engine encounters segmentation fault at `ips_bind_store`.
672345	IPS engine causes high memory usage.
675823	In NGFW policy-based mode, traffic does not pass through members of the zone with intrazone traffic allowed.
676322	Website fails in flow-based mode inspection.
679187	IPS engine swaps the root CA with FortiGate certificate while accessing some websites.
681345	FortiGate 1800F IPSA self test fails and disables IPSA log messages in the crash log.
683453	Floating point exception at `make_ftgd_re_eval_link` triggers IPS engine crash.
685676	URL filter does not match wildcard expression correctly while on flow-based inspection mode.
687449	IPS engine does not block/log traffic if an application is specified in security-policy in NGFW policy-based mode
688668	SSL mode switching from inline to dry run causes crash.
691395	Signature false positives cause outage after IPS database update.

Known issues

There are no known issues with this release of IPS engine version 6.2 for FortiOS.

To report a bug, please contact Customer Service & Support.